HIPAA Template Draft

- Title **INFORMATION SECURITY: RISK ANALYSIS AND MANAGEMENT**
- Creation
  - Date 02/22/01
  - Author Dana Kleiman/ Maria Dedet Mina Martel
  - Phone number 916/ 654-9381 916/ 654-2214
  - Email address dkleiman@edd.ca.gov mmartel@dds.ca.gov
- Revision
  - Date
  - Author
  - Phone number
  - Email address

I) Introduction

This is a template on developing Risk Analysis and Risk Management measures for the protection of data and information assets affected by HIPAA rules and regulations.

II) Purpose

HIPAA's Final Rule, Part 164 (Security and Privacy) mandates the protection of the confidentiality of individual medical data/records. This document acts as a guide for compliance with HIPAA requirements for the risk analysis and risk management of these information assets.

III) Assumptions, Pre-requisites, and Dependencies

A) "Each state department or state agency shall designate a position within the department or agency, the duties of which shall include, but not be limited to, responsibility for the privacy policy within that department or agency." –SB No. 129, Chapter 984: a position must be designated.

B) Responsibility for review and monitoring of plans will be under a department/ agency level Security Officer and/or Privacy Officer.

C) The Security Officer and/or Privacy Officer will have responsibility to coordinate with IT system administrators to establish authorities for access to confidential

data. Levels of access must be established for both employees and other authorized users of the information assets of the department or agency.

D) Policies and procedures to protect data will be designed and in place for each state department or agency. If State law is more stringent than Federal, State law will be followed.

E) Confidentiality Statement and/or Access Control Statement to be signed by the authorized user and/or owner of the data will be in place and part of regular security practices.

F) A system will be in place to report violations or incidents.

G) Sanctions for non-compliance will be part of the policies and procedures.

H) Training will occur at work unit level and at regular intervals to maintain employee security awareness.

I) All applicable laws, rules, regulations unique to each state agency will be included in development of their templates, business practices, policies and guidelines.

IV) Constraints

A) Time

1) Any deadline on meeting compliance requirements
2) Time available for review of work-unit plans or form submissions
3) Timing of reviews…how often, what time of year, etc.

B) Personnel

1) Are there agency Security Officers? Who else has authority?
2) Are there sufficient personnel to review work-unit plans/forms? Are they available?
3) Are their skill sets sufficient?

C) Resources

1) Materials
2) Facilities
3) Access
4) Authorities
5) Funding/ Budget
6) Personnel

D) Authorities

1) Security Officer
2) Privacy Officer
3) IT unit
4) Information Security Unit
5) Who has ultimate responsibility for program? To determine business need for authorities?
6) Who (or what position) will be the agency contact?
7) What controls are in place for actions of Covered Entities (Health Plans, Clearinghouses, Health Providers), Hybrid Entities, Affiliated Covered Entities and Business Associates (including Subcontractors and Agents)?
8) What are the legislative, regulatory or policy-related mandates specific to the operations and business practices of each agency or department?

V) Process

A) Identify and Evaluate

Each agency or department shall determine if it is affected by the HIPAA Rule. (see PSN's free internet HIPAA Calculator Report: http://www.privacysecuritynetwork.com/healthcare/hipaa/default. cfm. Also, refer to the Covered Entity template).

Each agency or department affected by the HIPAA Rule must:

1) identify the data or information asset to be protected, including systems, personnel and equipment.

2) determine the critical value/ risk level of the identified data or information asset (see SAM 4840.4: Definitions).

3) identify what may adversely affect the data or information asset.

4) determine acceptable risk levels based on probability of the event, probability of financial loss (including personnel hours) or legal action, and vulnerabilities of the organization.

B) Identify and Assign

Each agency or department affected by the HIPAA Rule shall:

1) identify and assign levels of risks in accordance with the information or data owned or maintained and the probability or severity of losses.

2) identify safeguards to reduce negative effects of data or information loss, modification, destruction or damage, misuse, or unauthorized access or disclosure and reduce the likelihood that such events will occur.

C) Plan

Each agency or department affected by the HIPAA Rule shall:

1) develop a plan for selecting and implementing cost-effective or critical safeguards.

2) develop policies, procedures, processes, standards and guidelines to support the protection and security of its data or information assets.

3) create, review or amend its existing Business Continuity Plan. Continuity Plans must include security measures for the protection of data or information assets affected by the HIPAA Rule.

D) Implement

Each agency or department affected by the HIPAA Rule shall:

1) develop and deliver security training to all employees, business partners and other data or information users, as appropriate.

2) institute and follow measures for the authorized destruction of data or information assets (e.g. tape swipes, paper shredders).

VI) Procedures

A) Identify and Evaluate

Each agency or department shall determine if the HIPAA Rule affects it (see PSN's free internet HIPAA Calculator Report: http://www.privacysecuritynetwork.com/healthcare/hipaa/default. cfm. Also, refer to the Covered Entity template).

1) If affected by the HIPAA Rule, the agency or department shall:

(a) identify the data or information asset to be protected, including systems, personnel and equipment (see SAM, Section 4840-4845).

(b) create a checklist which identifies risks and vulnerabilities involved in the release of information to a variety of users (see Attachment No. 1 – Risk Analysis Questionnaire).

(c) assign a critical value/ risk level to the data or information asset based on the risks and vulnerabilities identified.

2) Procedures useful in the identification and evaluation of risk are:
   (d) Brainstorming
   (e) Physical, logical or theoretical walk-throughs of a process, system, life cycle or facility
   (f) Flowcharts of procedure or process flows, floor plans, network or system configurations, etc.
   (g) Review of historical information, including evaluations, audits, compliance reviews, issue memos, incident reports generated during the normal course of business.
   (h) Use of existing internal materials, externally published materials and internet sites which deal with the subjects of risk analysis and risk management.

B) Identify and Assign

1) Each agency or department shall create a list of possible consequences to support the determination of risk level (see Attachment No. 2 – Listing of Consequences).

2) Determination of risk level and consideration of acceptable risk should be based on:
   (a) Probability of a risk's occurrence
   (b) Percentage of likelihood
   (c) Ratio
   (d) Number of occurrences within a specified time period
   (e) Value
   (f) Loss Hours (increase in staff hours if event occurs)
   (g) Cost of Loss Hours
   (h) Consequences
   (i) Financial loss
   (j) Liability
   (k) Bad publicity
   (l) Loss of credibility or public trust
   (m) Loss of life or injury
   (n) Impact on workload, personnel or facilities
   (o) Impact on ability to meet federal and/or state legislative mandates

3) Each agency or department shall review its existing practices and identify where security of information assets (including but not limited to, systems, personnel and equipment,) may be improved.

4) An additional tool for Risk Management is DOIT's Risk Management Plan (http://www.doit.ca.gov/SIMM/Project Management/docs/sb5rmw.doc).

C) Plan

1) Each agency or department shall create, alter or amend existing security policies, procedures, guidelines and practices to include security considerations for the protection of HIPAA sensitive or confidential information (see Attachment No. 3 – Summary of British Standard 7799 – 1:1999).

2) Each agency or department shall research safeguards and methods to mitigate identified risks and vulnerabilities specific to HIPAA (e.g. Attachment No.. 4 – Data Handling Matrix). Some safeguards to be considered are:
   (a) computer programs and controls
   (b) authenticaton
   (c) access authorizations
   (d) firewalls
   (e) equipment and facility access controls
   (f) personnel practices
   (g) security in the workstations (direction of monitors, etc.)
   (h) security awareness training

3) A plan should be developed to implement those safeguards and mitigations which are most cost effective or which are critical.

4) Each agency or department shall develop a Business Continuity Plan to address security concerns in the event of a disaster which shall consist of both an Emergency Response Plan and a Business Resumption Plan.

D) Implement

1) Each agency or department shall institute practices to reduce security risks and shall review them periodically.

2) Each agency or department should perform a "dry run" of their Business Continuity Plan on an annual basis.

VII) Information Concerns

A) **Confidentiality** – secure information from unauthorized disclosure

B) **Integrity** – safeguard the accuracy and completeness of data and information

C) **Availability** – ensure information assets are available when required

VIII) Monitoring compliance criteria

A) Accountability

1) What are the levels of accountability?
2) Individual positions should be assigned for the following levels of responsibility:
   (a) Creation of the policies, standards, practices, procedures and guidelines which protect the security of HIPAA sensitive or confidential data or information assets
   (b) Implementation of those policies, standards, practices, procedures and guidelines
   (c) Maintenance of those policies, standards, practices, procedures and guidelines
   (d) Monitoring of compliance with those policies, standards, practices, procedures and guidelines
   (e) Enforcement of those policies, standards, practices, procedures and guidelines

B) **Enforcement:**

1) Federal
   (a) **HIPAA** - go to website: **_____reference_____**
   (b) Also refer to:
      (1) Federal Privacy Act
      (2) Federal Computer Fraud Act
      (3) Freedom of Information Act
      (4) Law 42 USC Section 503 of the Social Security Act

2) State
   (a) **SB19** - go to website: **_____reference_____**
   (b) Also refer to:
      (1) Information Practices Act (Civil Code Section 1798)
      (2) Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502)
      (3) Public Records Act (Government Code Section 6250)
      (4) the SAM
      (5) the California Unemployment Insurance Code (Section 2714) provides guidelines for Disability Insurance disclosure of medical information.

IX) Glossary of terms

Go to website: **_____reference_____**